

The Cauchy-Davenport Theorem for Finite Groups

Jeffrey Paul Wheeler*

February 2006

Abstract

The Cauchy-Davenport theorem states that for any two nonempty subsets A and B of $\mathbb{Z}/p\mathbb{Z}$ we have $|A+B| \geq \min\{p, |A|+|B|-1\}$, where $A+B := \{a+b \bmod p \mid a \in A, b \in B\}$. We generalize this result from $\mathbb{Z}/p\mathbb{Z}$ to arbitrary finite (including non-abelian) groups. This result from early in 2006 is independent of Gyula Károlyi's¹ 2005 result in [15] and uses different methods.

1 Background and Motivation

The problem we will be considering lies in the area of Additive Number Theory. This relatively young area of Mathematics is part of Combinatorial

*Department of Mathematics, the University of Pittsburgh, Pittsburgh PA 15260, USA.
E-mail: jwheeler@pitt.edu.

¹Gyula was a visitor at the University of Memphis early in my time as a graduate student there. I wish to thank him for introducing me to this problem and encouraging me to work on it (in addition to teaching a great class on the subject). Regrettably I did not inform Gyula that I was working on the problem and that progress was being made, hence the independent results. I discovered Gyula had a result the day before presenting the work to the Combinatorics seminar at the University of Memphis (which was incredibly disappointing to a graduate student with his first result).

Number Theory and can best be described as the study of sums of sets of integers. As such, we begin by stating the following definition:

Definition 1.1. *For subsets A and B of a group G , define*

$$A + B := \{a + b \mid a \in A, b \in B\}$$

where $+$ is the group operation. We write

$$A \cdot B := \{ab \mid a \in A, b \in B\}$$

in the case when the group G is written multiplicatively.

A simple example of a problem in Additive Number Theory is given two subsets A and B of a set of integers, what facts can we determine about the sumset $A + B := \{a + b \mid a \in A, b \in B\}$? The topic of this paper is one such problem. Note that a very familiar problem in Number Theory, namely Lagrange's theorem that every nonnegative integer can be written as the sum of four squares, can be expressed in terms of sumsets. In particular,

Theorem 1.2. *[Lagrange's Four Square Theorem]*

Let $\mathbb{N}_0 = \{x \in \mathbb{Z} \mid x \geq 0\}$ and let $\mathbb{S} = \{x^2 \mid x \in \mathbb{Z}\}$. Then

$$\mathbb{N}_0 = \mathbb{S} + \mathbb{S} + \mathbb{S} + \mathbb{S}.$$

As well the the binary version of Goldbach's Conjecture can be restated in terms of sumsets.

Conjecture 1.3. *[Goldbach's Conjecture]*

Let $\mathbb{E} = \{2x \mid x \in \mathbb{Z}, x \geq 2\}$ and let $\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ is prime}\}$. Then

$$\mathbb{E} \subseteq \mathbb{P} + \mathbb{P}. \tag{1}$$

In other words, every even integer is greater than 2 is the sum of two primes. Notice that we do not have set equality in equation (1) because $2 \in \mathbb{P}$.

The theorem we wish to extend was first proved by Augustin Cauchy in 1813² [3] and later independently reproved by Harold Davenport in 1935 [5] (Davenport discovered in 1947 [6] that Cauchy had previously proved the theorem.) In particular,

²Cauchy used this theorem to prove that $Ax^2 + By^2 + C \equiv 0(\text{mod } p)$ has solutions provided that $ABC \not\equiv 0$. This is interesting in that Lagrange used this result to establish his four squares theorem.

Theorem 1.4 (Cauchy-Davenport). *If A and B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, p prime, then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

We note that in 1935 Inder Chowla [4] extended the result to composite moduli m when $0 \in B$ and the other members of B are relatively prime to m . As well it is worth noting that in 1996 Alon, Nathanson, and Ruzsa provided a simple proof of this theorem using the Polynomial Method [1].

Of interest to this work is Gyula Károlyi's extension of the theorem to abelian groups [13, 14]. Before we state the theorem, though, a useful definition:

Definition 1.5 (Minimal Torsion Element). *Let G be a group. We define $p(G)$ to be the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$ (or, if multiplicative notation is used, $g^p = 1$, $g \neq 1$). If no such p exists, we write $p(G) = \infty$.*

Lemma 1.6. *For any finite group $G \neq \{1\}$, $p(G)$ is the smallest prime factor of $|G|$.*

Proof. Let p be the smallest prime dividing $|G|$. Then by Cauchy's Theorem, there is an element $g \in G$ of order p , i.e., $g^p = 1$ but $g \neq 1$. Suppose there were a smaller prime q with $h^q = 1$, $h \neq 1$. Then $|\langle h \rangle| = q$ and by Lagrange's Theorem $q \mid |G|$. This contradicts the choice of p . \square

Now we state the generalization of Theorem 1.4 to abelian groups.

Theorem 1.7 (Károlyi [13, 14]). *If A and B are nonempty subsets of an abelian group G , then $|A + B| \geq \min\{p(G), |A| + |B| - 1\}$.*

Before we continue we state a famous and very useful result.

Theorem 1.8 (Feit-Thompson [12]). *Every group of odd order is solvable.*

Since any group G of even order has $p(G) = 2$, we will mainly be considering groups of odd order. Hence by Theorem 1.8, we will mainly be considering only solvable groups.

2 A Basic Structure of Finite Solvable Groups

Throughout this section G will be a finite solvable group, i.e., there exists a chain of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_{i-1} is a normal subgroup of G_i and the quotient group G_i/G_{i-1} is abelian for $i = 1, 2, \dots, n$.

Hence by definition, either $G = \{1\}$, or there is some proper normal subgroup $K \triangleleft G$ such that K is also solvable and the quotient group G/K is abelian. (In fact for finite groups one can also insist that G/K is cyclic of prime order, i.e., isomorphic to some $\mathbb{Z}/p\mathbb{Z}$, p prime. However we shall not require this.)

Fix for each coset $h \in G/K$ a representative $\tilde{h} \in G$, so that $\tilde{h} \in h$ and $h = K\tilde{h} \in G/K$. Each $g \in G$ lies in a unique coset $h \in G/K$, and then $g\tilde{h}^{-1}$ lies in K . Thus there is a $k \in K$ and an $h \in G/K$ such that $g = k\tilde{h}$. The pair (k, h) is unique since if $g = k\tilde{h} = k'\tilde{h}'$ then $Kg = h = h'$ and then $k = g\tilde{h}^{-1} = k'$. Define

$$\psi: G \rightarrow K \times G/K \quad \text{by } \psi(g) = (k, h), \quad \text{where } g = k\tilde{h}. \quad (2)$$

Then ψ is a bijection between the sets G and $K \times G/K$. Define an operation \star on $K \times G/K$ by

$$(k_1, h_1) \star (k_2, h_2) := (k_1\phi_{h_1}(k_2)\eta_{h_1, h_2}, h_1h_2).$$

where $\phi_h \in \text{Aut}(K)$ is defined by $\phi_h(k) = \tilde{h}k\tilde{h}^{-1} \in K$ (recall $K \trianglelefteq G$), and

$$\eta_{h_1, h_2} = \tilde{h}_1 \cdot \tilde{h}_2 \cdot (\widetilde{h_1h_2})^{-1} \in K. \quad (3)$$

Note that both ϕ_h and η_{h_1, h_2} depend on the choice of coset representatives of G/K . As will be seen in the examples, η plays a role analogous to “carrying the one” in simple arithmetic.

Lemma 2.1 (Basic Structure of Solvable Groups). *Let G be a solvable group with $K \trianglelefteq G$. Upon fixing the set $R = \{\tilde{h} \mid h \in G/K\}$ of coset representatives of G/K , ψ in (2) is an isomorphism from G to the group $(K \times G/K, \star)$.*

Proof. As noted above, ψ is a bijection, so it is enough to show it is a homomorphism. Suppose that $g_1 = k_1\tilde{h}_1$ and $g_2 = k_2\tilde{h}_2$. Then

$$\begin{aligned}
\psi(g_1) \star \psi(g_2) &= (k_1, h_1) \star (k_2, h_2) \\
&= (k_1\phi_{h_1}(k_2)\eta_{h_1, h_2}, h_1h_2) \\
&= (k_1\tilde{h}_1k_2\tilde{h}_1^{-1}\tilde{h}_1\tilde{h}_2(\widetilde{h_1h_2})^{-1}, h_1h_2) \\
&= \psi(k_1\tilde{h}_1k_2\tilde{h}_2(\widetilde{h_1h_2})^{-1}\widetilde{h_1h_2}) \\
&= \psi(k_1\tilde{h}_1k_2\tilde{h}_2) \\
&= \psi(g_1g_2)
\end{aligned}$$

□

It is worth noting that the construction of \star on $K \times G/K$ is more general than the semi-direct product of two groups. Indeed, G may not be a semi-direct product of K and G/K . If however it is, then one can choose the representatives \tilde{h} so that $\eta_{h_1, h_2} = 1$ for all $h_1, h_2 \in G/K$.

Before we continue, consider two illustrative examples.

Example 2.2. Let p be a prime, $G = \mathbb{Z}/p^2\mathbb{Z}$ and $K = p\mathbb{Z}/p^2\mathbb{Z}$. Let the representatives of G/K be $\{0, 1, \dots, p-1\} \pmod{p^2}$. Then we can represent G as a set of pairs $(ap, b+K)$, $a, b \in \{0, 1, \dots, p-1\}$ (or more simply as just (a, b) , see Table 1). The automorphism ϕ_{b+K} is the identity as G is abelian. However, $\eta(b+K, d+K) = (b \bmod p) + (d \bmod p) - (a+b \bmod p)$ which is $0 \in K$ when $b+d < p$ and $p \in K$ when $b+d \geq p$. Hence addition in G is given by $(a, b) + (c, d) = (a+b+\eta \bmod p, b+d \bmod p)$ where $\eta = 0$ if $b+d < p$ and 1 if $b+d \geq p$. However, this is effectively just “addition with carry” of two digit base p numbers.

Table 1: Elements $g \in \mathbb{Z}/p^2\mathbb{Z}$ represented as pairs $\phi(g) = (a, b)$, $a, b \in \{0, \dots, p-1\}$.

g	0	1	\dots	$p-1$	p	$p+1$	\dots	p^2-1
$\psi(g)$	$(0, 0)$	$(0, 1)$	\dots	$(0, p-1)$	$(1, 0)$	$(1, 1)$	\dots	$(p-1, p-1)$

Example 2.3. Let Q be the quaternion group, namely $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ where $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ and $i^2 = j^2 = k^2 = -1$. Put $K = \{\pm 1, \pm k\}$, so that $Q/K = \{K, Kj\}$ and we choose 1 as our coset representative of K and j as the coset representative of Kj

The order of Kj in Q/K is 2 however the order of j in Q is 4. Indeed

$$\eta_{Kj, Kj} = j \cdot j \cdot 1^{-1} = j^2 = -1$$

since the coset representative of $(Kj)^2 = K$ is 1.

Thus, since $i = -k \cdot j$,

$$\begin{aligned} \psi(i \cdot i) &= (-k, Kj)(-k, Kj) \\ &= (-k(j(-k)j^{-1})\eta_{j,j}), (Kj)^2 \\ &= (-k(k)(-1), K) \\ &= (-1, K) = \psi(-1) \end{aligned}$$

Which is what we hoped for since $i \cdot i = -1$.

Table 2: Elements of Q written as pairs with coset representatives 1 and j .

$g \in Q$	1	-1	i	$-i$	j	$-j$	k	$-k$
$\psi(g)$	$(1, K)$	$(-1, K)$	$(-k, Kj)$	(k, Kj)	$(1, Kj)$	$(-1, Kj)$	(k, K)	$(-k, K)$

This basic structure is sufficient for tackling the job of establishing the Cauchy-Davenport Theorem for finite groups. It is worth mentioning that a more sophisticated structure for solvable groups is required for proving the related problem of Erdős and Heilbronn (see [2]). As well, we note that neither $\mathbb{Z}/p^2\mathbb{Z}$ nor the quaternion group is a semidirect product of its respective K and G/K .

Before proceeding, developing some notation will be helpful.

Definition 2.4. Let G be a finite solvable group and $K \triangleleft G$. For $S \subseteq G$, represent S as a subset $\psi(S) = \{\psi(g) \mid g \in S\}$ of $K \times G/K$ as above and

write

$$\begin{aligned} S^1 &:= \{k \in K \mid \exists h \in G/K : (k, h) \in \psi(S)\}, \\ S^2 &:= \{h \in G/K \mid \exists k \in K : (k, h) \in \psi(S)\}. \end{aligned}$$

In other words, S^1 is the collection of first coordinates and S^2 is the collection of second coordinates of the elements of $\psi(S)$.

3 The Cauchy-Davenport Theorem for Finite Solvable Groups

Theorem 3.1. *Suppose G is a finite solvable group and A, B are non-empty subsets of G . If $|A| + |B| - 1 \leq p(G)$, then $|A \cdot B| \geq |A| + |B| - 1$.*

Proof. We will proceed by induction on $|G|$. The result is trivial for $|G| = 1$ (note $p(\{1\}) = \infty$), so assume $|G| > 1$. As previously stated, there exists a $K \triangleleft G$ so that G/K is abelian, $K \neq G$, and K is solvable.

Let A and B be non-empty subsets of G . Write A and B as subsets of $(K, G/K)$ as above. Let $A^2 = \{h_1, \dots, h_\alpha\}$ and $B^2 = \{h'_1, \dots, h'_\beta\}$. For $i = 1, \dots, \alpha$, write

$$A_i = \{(k, h) \in \psi(A) \mid h = h_i\}, \quad a_i = |A_i|$$

and similarly for B_j , $b_j = |B_j|$, $j = 1, \dots, \beta$. Assume the h_i and h'_j are ordered so that

$$a_1 \geq a_2 \geq \dots \geq a_\alpha, \quad b_1 \geq b_2 \geq \dots \geq b_\beta.$$

We shall also assume without loss of generality that $\alpha \leq \beta$. Note that $\psi(A) = \bigcup_i A_i$, $\psi(B) = \bigcup_j B_j$, and

$$|A| = a_1 + a_2 + \dots + a_\alpha, \quad |B| = b_1 + b_2 + \dots + b_\beta.$$

If $(k, h_i) \in A_i$ and $(k', h'_j) \in B_j$, then

$$(k, h_i) \star (k', h'_j) = (k\phi_{h_i}(k')\eta_{h_i, h'_j}, h_i h'_j)$$

Thus, as h_i and h'_j are constant for all elements in A_i and B_j respectively,

$$|A_i \cdot B_j| = |(A_i \cdot B_j)^1| = |A_i^1 \cdot B'_j|$$

where $B'_j = \{\phi_{h_i}(k')\eta_{h_i, h'_j} \mid (k', h'_j) \in B_j\} \subseteq K$. Note that $|B'_j| = |B_j|$ as ϕ_{h_i} is an automorphism of K and multiplication by the constant η_{h_i, h'_j} does not change the size of the set. But K is solvable and $|G| = |K||G/K|$ so $a_i + b_j - 1 \leq |A| + |B| - 1 \leq p(G) \leq p(K)$. Hence by induction,

$$|A_i \cdot B_j| = |A_i^1 \cdot B'_j| \geq a_i + b_j - 1.$$

Now $A^2, B^2 \subseteq G/K$ and $|G| = |K||G/K|$, so $\alpha + \beta - 1 \leq |A| + |B| - 1 \leq p(G) \leq p(G/K)$. Hence by Theorem 1.7 (or by Theorem 1.4 if we insist that G/K is cyclic of prime order),

$$|A^2 \cdot B^2| = |\{h_i h'_j \mid 1 \leq i \leq \alpha, 1 \leq j \leq \beta\}| \geq \alpha + \beta - 1.$$

Now $\alpha + \beta - 1 = (\beta) + (\alpha - 1)$, so there are at least $\alpha - 1$ elements $h_i h'_j$ that are not one of the β distinct elements $h_1 h'_1, h_1 h'_2, \dots, h_1 h'_\beta \in G/K$. In particular, $|A \cdot B|$ contains at least $\alpha - 1$ elements that are not in any $A_1 \cdot B_j$. Since the second coordinate of every element of $A_1 \cdot B_j$ is $h_1 h'_j$, the sets $A_1 \cdot B_j$ are disjoint. Thus

$$\begin{aligned} |A \cdot B| &\geq |A_1 \cdot B_1| + |A_1 \cdot B_2| + \dots + |A_1 \cdot B_\beta| + \alpha - 1 \\ &\geq \sum_{j=1}^{\beta} (a_1 + b_j - 1) + \alpha - 1 \\ &= \beta a_1 + |B| - \beta + \alpha - 1 \\ &\geq |A| + |B| - 1, \end{aligned}$$

where in the last line we have used the fact that $\beta \geq \alpha$, and $\beta a_1 \geq \alpha a_1 = \sum_{i=1}^{\alpha} a_1 \geq \sum_{i=1}^{\alpha} a_i = |A|$. \square

4 The Cauchy-Davenport Theorem for Finite Groups

We now extend Theorem 3.1 to all finite groups.

Theorem 4.1. *Let G be a finite group and let A and B be non-empty subsets of G . Then $|A \cdot B| \geq \min\{p(G), |A| + |B| - 1\}$.*

Proof. If G is of even order then $p(G) = 2$. The result is then trivial as $|A \cdot B| \geq 2 = p(G)$ if either $|A| > 1$ or $|B| > 1$, while $|A \cdot B| = 1 = |A| + |B| - 1$ if $|A| = |B| = 1$. If G is of odd order then by Theorem 1.8, G is solvable. The result then follows from Theorem 3.1 when $|A| + |B| - 1 \leq p(G)$. If $|A| + |B| - 1 > p(G)$, take non-empty subsets $A^* \subseteq A$, $B^* \subseteq B$ such that $|A^*| + |B^*| - 1 = p(G)$. Then $|A \cdot B| \geq |A^* \cdot B^*| = p(G)$. \square

5 Closing Remarks

A problem closely related to the Cauchy-Davenport Theorem was the conjecture Paul Erdős and Hans Heilbronn posed in the early 1960s. Namely, if the addition in the Cauchy-Davenport Theorem is restricted to distinct elements, the lower bound changes only slightly. Erdős stated this conjecture in 1963 during a number theory conference at the University of Colorado [8]. Interestingly, Erdős and Heilbronn did not mention the conjecture in their 1964 paper on sums of sets of congruence classes [11] though Erdős mentioned it often in his lectures (see [18], page 106). Eventually the conjecture was formally stated in Erdős' contribution to a 1971 text [9] as well as in a book by Erdős and Graham in 1980 [10]. In particular,

Theorem 5.1 (Erdős-Heilbronn Problem). *If A and B are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime, then $|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}$, where $A \dot{+} B := \{a + b \bmod p \mid a \in A, b \in B \text{ and } a \neq b\}$.*

The conjecture was first proved for the case $A = B$ by Dias da Silva and Hamidoune in 1994 [7] with the more general case established by Alon, Nathanson, and Ruzsa using the polynomial method in 1995 [1]. Károlyi extended this result to abelian groups for the case $A = B$ in 2004 [14] and to cyclic groups of prime powered order in 2005 [17].

A more general result of the Erdős-Heilbronn Problem for finite groups is established in [2].

References

- [1] Noga Alon, Melvyn B. Nathanson, and Imre Ruzsa, The polynomial method and restricted sums of congruence classes, *Journal of Number Theory* **56** (1996) 404–417.
- [2] Paul Balister and Jeffrey Paul Wheeler, The Erdős-Heilbronn problem for finite groups, to appear in *Acta Arithmetica*.
- [3] A. Cauchy, Recherches sur les nombres, *J. École Polytech* **9** (1813), 99–116.
- [4] Inder Chowla, A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring’s problem, *Proceedings of the Indian Academy of Sciences, Section A*, **1**, (1935) 242–243.
- [5] H. Davenport, On the addition of residue classes, *Journal of the London Mathematical Society* **10** (1935), 30–32.
- [6] H. Davenport, A historical note, *Journal of the London Mathematical Society* **22** (1947), 100–101.
- [7] Dias da Silva, J.A. and Hamidoune, Y.O., Cyclic spaces for Grassmann derivatives and additive theory, *The Bulletin of the London Mathematical Society* **26** (1994) 140–146.
- [8] Erdős, P., On the addition of residue classes (mod p), *Proceedings of the 1963 Number Theory Conference at the University of Colorado*, Univeristy of Colorado Press, (1963) 16–17.
- [9] Erdős, P., Some problems in number theory, in *Computers in number theory*, edited by A.O.L. Atkin and B.J. Birch, Academic Press, (1971) 405–414.
- [10] Erdős, P. and Graham, R.L., Old and new problems and results in combinatorial number theory. Monographies de L’Enseignement Mathématique [Monographs of L’Enseignement Mathématique] **28** Université de Genève *L’Enseignement Mathématique*, 1980, 128pp.
- [11] Erdős, P. and Heilbronn, H., On the addition of residue classes (mod p), *Acta Arithmetica* **9** (1964) 149–159.

- [12] Walter Feit and John G. Thompson, Solvability of groups of odd order, *Pacific Journal of Mathematics* **13** (1963) 775–1029.
- [13] Gyula Károlyi, On restricted set addition in abelian groups, *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Mathematica*, **46** (2003), 47–53.
- [14] Gyula Károlyi, The Erdős-Heilbronn problem in abelian groups, *Israel Journal of Mathematics* **139** (2004), 349–359.
- [15] Gyula Károlyi, The Cauchy-Davenport theorem in group extensions, *L'Enseignement Mathématique* **51** (2005), 239–254.
- [16] Gyula Károlyi, An inverse theorem for the restricted set addition in abelian groups, *Journal of Algebra* **290** (2005), 557–593.
- [17] Gyula Károlyi, A compactness argument in the additive theory and the polynomial method, *Discrete Mathematics* **302** (2005), 124–144.
- [18] Nathanson, Melvyn B., *Additive number theory, inverse problems and the geometry of subsets*, Springer-Verlag, 1996.